Table of Contents

LevelBlue Endpoint Security with SentinelOne

Section Effective Date: 09-Apr-2024

LevelBlue Endpoint Security with SentinelOne (the Service) is made up of the following Service Components:

- Endpoint Security - Control
- Endpoint Security - Complete
- Mobile Security
- Active Directory Defense
- Identity Threat Detection and Response

The LevelBlue Endpoint Security with SentinelOne Service Guide consists of the following:

- Service Description (SD)
- Service Level Objectives (SLO)
- Pricing (P)
- Country Specific Provisions (CSP)

In addition, specified portions of the General Provisions apply.

Service Description (SD)

SD-1. LevelBlue Endpoint Security with SentinelOne – Control Overview

Section Effective Date: 25-Mar-2023

LevelBlue Endpoint Security with SentinelOne - Control (Endpoint Security - Control) unifies malware prevention, detection, and remediation in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and visibility into the endpoint environment with full-context, near real-time forensics.

The features of Endpoint Security - Control are:

- SentinelOne Endpoint Agent
- SentinelOne Management Platform

SD-1.1. Service Features

SD-1.1.1. SentinelOne Endpoint Agent – Control

Section Effective Date: 12-Dec-2023

The SentinelOne Endpoint Agent provides real-time, autonomous detection and remediation of malicious activity on a host with its behavioral AI pre-execution and reputation engines. It also provides local host firewall control, Bluetooth/USB control, and audit. The SentinelOne Endpoint Agent packages are:

- Endpoint Security Control is available for designated versions of Windows, macOS, and Linux devices or servers
- Endpoint Security Control K8s is available for containers, and cloud-native workloads and may be utilized for endpoint and container telemetry and log collection from assets directly as well as on an ad-hoc basis for forensic analysis and response activities

SD-1.1.2. SentinelOne Management Platform

Section Effective Date: 07-Oct-2021

The SentinelOne Management Platform includes the cloud database of threat intelligence and a browser-based management console that communicates with the SentinelOne Endpoint Agent. The management console is used to manage endpoints and end users, track actions, analyze data, and mitigate threats with quick incident response. The SentinelOne Management Platform includes the following features:

SD-1.1.2.1. SentinelOne Platform Management Console

Section Effective Date: 07-Oct-2021

The SentinelOne Platform Management Console can be accessed 24x7x365 using two-factor authentication.

SD-1.1.2.2. Full Disk Scans

Section Effective Date: 07-Oct-2021

Full Disk Scans can be run on the SentinelOne Endpoint Agent to find dormant malicious files on the hard disk and compliance violations. The scan inspects file headers of numerous file types and local file system, but not network drives which would require user credentials.

SD-1.1.2.3. Firewall Control

Section Effective Date: 07-Oct-2021

Firewall Control manages endpoint firewall settings from the Management Console. This is used to define which network traffic, application connections, and other connections are allowed in and out of endpoints. The firewall rules are sent to Agents from the Management Console. This feature works only for certain operating systems, which will be determined prior to Service implementation.

SD-1.1.2.4. Device Control

Section Effective Date: 07-Oct-2021

Device Control allows customers to control which external devices are allowed to be used with endpoints, e.g., USB, Bluetooth.

SD-1.1.2.5. Asset Discovery

Section Effective Date: 07-Oct-2021

The Asset Discovery feature is used to detect new devices in Customer's environment and provides an asset inventory of Windows, macOS, and Linux assets which have or have not had the Agent installed. Assets can be assigned to static and dynamic groups, allowing customers to group assets with specific security or audit needs for ease of reporting.

SD-1.1.2.6. Application Vulnerability

Section Effective Date: 07-Oct-2021

The Application Vulnerability feature executes a query on the OS and collects all the applications that are installed and registered on that asset. The SentinelOne Management Platform will query MITRE for any open CVEs related to the versions of the discovered applications to identify any vulnerabilities.

SD-2. LevelBlue Endpoint Security with SentinelOne – Complete Overview

Section Effective Date: 12-Dec-2023

LevelBlue Endpoint Security with SentinelOne - Complete (Endpoint Security - Complete) includes the capabilities in Endpoint Security – Control and adds the following capabilities:

SD-2.1. SentinelOne Endpoint Agent-Complete

Section Effective Date: 12-Dec-2023

The SentinelOne Endpoint Agent provides real-time, autonomous detection and remediation of malicious activity on a host with its behavioral AI, pre-execution and reputation engines. It also provides local host firewall control, Bluetooth/USB control and audit. The SentinelOne Endpoint Agent packages are:

- Endpoint Security Complete is available for designated versions of Windows, macOS, and Linux devices or servers.
- Endpoint Security Complete K8s is available for containers, and cloud-native workloads and may be utilized for endpoint and container telemetry and log collection from assets directly as well as on an ad-hoc basis for forensic analysis and response activities.

SD-2.2. Deep Visibility

Section Effective Date: 07-Oct-2021

The Deep Visibility feature utilizes the built-in behavioral analysis engine to collect an array of benign meta-data for use by threat hunters and analysts across the entire enterprise. Deep Visibility queries collect additional information on related processes, files, URLs, DNS, IP, login, registry keys, scheduled tasks, full disk scan results, and behavioral indicators. Deep Visibility data is retained on the SentinelOne Management platform for 14 days.

SD-3. LevelBlue Mobile Security with SentinelOne Overview

Section Effective Date: 12-Dec-2023

LevelBlue Mobile Security with SentinelOne is a Mobile Threat Defense (MTD) solution that utilizes AI detection engines to detect malicious behavior, host attacks, and network attacks on mobile devices. Mobile Security also utilizes Behavioral AI to detect threats through evasion techniques.

The features of Mobile Security with SentinelOne are:

- SentinelOne Mobile Agent
- SentinelOne Management Platform

SD-3.1. SentinelOne Mobile Agent

Section Effective Date: 25-Mar-2023

The SentinelOne Mobile Agent provides Mobile Security support for iOS, Android, and ChromeOS devices. The SentinelOne Mobile Agent detects mobile malware with behavioral based AI, phishing with real time link and content analysis, network threats via advanced scanning, and device vulnerability detection to alert on jailbroken devices, devices without PINs, CVEs, and more.

SD-3.2. SentinelOne Mobile Management Platform

Section Effective Date: 12-Dec-2023

The SentinelOne Mobile Management Platform includes the cloud database of threat intelligence and a browser-based management console that communicates with the SentinelOne Mobile Agent. The management console is used to manage mobile endpoints and end users, track actions, analyze data, and mitigate threats with quick incident response. The SentinelOne Mobile Management Platform includes access to the SentinelOne Platform Mobile Management Console.

SD-4. LevelBlue Active Directory Defense with SentinelOne Overview

Section Effective Date: 09-Apr-2024

LevelBlue Active Directory Defense with SentinelOne is an identity configuration assessment that identifies misconfigurations, vulnerabilities, and attack indicators within Active Directory (AD) and Azure AD and detects active attacks aimed at on-premises AD controllers.

SD-4.1. AD Connector Agent

Section Effective Date: 09-Apr-2024

The AD Connector Agent must be installed on one Adjoined Windows endpoint to complete scans of the AD to identify exposures. Once configured in the SentinelOne Identity Management Platform the ADSecure-DC module will be deployed to any Domain Controllers to detect any attacks against AD and creates alerts, blocking access or requires re-authenticating with MFA when risky behavior is observed.

SD-4.2. SentinelOne Identity Management Platform-ADSecure-DC

Section Effective Date: 09-Apr-2024

The SentinelOne Identity Management Platform includes a cloud database and a browser-based management console that communicates with the Domain Controllers to identify Active Directory attacks. The management console is used to configure the Active Directory, report out any exposures, and define the actions to be triggered from Active Directory exposures.

SD-5. LevelBlue Identity Threat Detection and Response with SentinelOne Overview

Section Effective Date: 09-Apr-2024

LevelBlue Identity Threat Detection and Response (ITDR) with SentinelOne defends in real time domain-joined endpoints from adversaries aiming to gain privilege and move covertly.

The features of Identity Threat Detection and Response are:

- Identity Agent
- SentinelOne Identity Management Platform

SD-5.1. Identity Agent

Section Effective Date: 09-Apr-2024

The Identity Agent is installed on all endpoints and is available for designated versions of Windows, macOS, and Linux devices or servers. The Identity Agent completes queries to identify misuse and reconnaissance activity happening within endpoint processes and uploads the details of these queries to the SentinelOne Identity Management Platform for correlation and reporting purposes. On-agent cloaking, and deception techniques slow the adversary down while providing situational awareness.

SD-5.2. SentinelOne Identity Management Platform-ADSecure-EP

Section Effective Date: 09-Apr-2024

The SentinelOne Identity Management Platform includes a cloud database and a browser-based management console that communicates with the Identity Agents. The management console is used to configure module settings. create policies or rules, view alerts or events, and create deception objects. The SentinelOne Identity Management Platform includes the following modules:

SD-5.2.1. ADSecure-EP

Section Effective Date: 09-Apr-2024

ADSecure-EP first identifies AD lookups from untrusted applications, users, and computers. Then, ADSecure- EP removes the real AD objects in the response and inserts decoy objects. ADSecure-EP not only protects the production AD from attackers but also deceives them with the decoys.

SD-5.2.2. ThreatPath

Section Effective Date: 09-Apr-2024

The ThreatPath analysis engine in the Identity management console collects and correlates the data sent by each Identity Agent to detect potential lateral-movement paths, show critical AD objects, show the production and deceptive credential on endpoints, and remediate the detected exposures.

SD-5.2.3. Deflect

Section Effective Date: 09-Apr-2024

With Deflect every endpoint on the network becomes a decoy to deflect incoming and outgoing connection attempts. Failed inbound or outbound connections can be deflected by rules that trigger connections to be redirected.

SD-5.2.4. ThreatStrike

Section Effective Date: 09-Apr-2024

ThreatStrike are deceptive tokens or clues that you can configure on your endpoints to create a false trail that leads attackers away from your real assets. These tokens are the usual data such as user credentials, browser credentials, browser cookies, email client credentials, secure shell credentials, Windows Remote Desktop credentials, and so on. When attackers consume these deceptive tokens during lateral movement, events are raised in the Identity management console.

SD-6. Endpoint Security General Services

SD-6.1. Customer Training

Section Effective Date: 07-Oct-2021

As part of the purchase of the Service, Customer will be provided:

- One training seat to the SentinelOne 1-day training class. Additional training seats can be purchased at Customer's discretion.

SD-6.2. Endpoint Security Supported Endpoint List

Section Effective Date: 07-Oct-2021

Only the endpoint types and endpoint quantities previously reviewed and approved by LevelBlue will be included in the Service. Any changes to the endpoint types or endpoint quantities will require additional review and approval by LevelBlue. If the scope of deployment leads to a subscription tier change for the number of endpoints, Customer will be responsible for any adjustments to pricing as set forth in the Service Agreement. Customer changes to the number of endpoints must be provided in writing to LevelBlue within ten (10) business days prior to such change(s) taking effect.

SD-6.3. Support Availability

Section Effective Date: 25-Mar-2023

The following scope of Technical Support is available to Customers 24x7:

- Providing instruction on best practices for use and operation of the product
- Receiving and recording requests to enhance existing, or to implement new product functionality
- Receiving and recording requests for third party integration with the product.
- Identifying, analyzing, and accepting reports of product defects
- Providing work arounds to identified product defects or feature gaps when available
- Assist customers in identifying, analyzing, and resolving product challenges that prevent intended and designed functionality

SD-7. Reporting

Section Effective Date: 25-Mar-2023

Reports are provided via the SentinelOne Platform Management Console. Automated reports include:

- Executive Insights – show trends for threats, risks, and deployments
- Executive Insights by Group – show trends for threats, risks, and deployments for a specified asset group
- Threat Insights – show details on how threats were detected, at what confidence level, actions taken, and more threat and risk details
- Mitigation & Response Insights – show mitigation actions and trends
- Application Insights – provide information that Endpoint Agents collect about installed and executed applications

SD-8. Customer Responsibilities

Section Effective Date: 25-Mar-2023

Customer is required to:

- Assign a Single Point of Contact ("SPOC") to provide Customer Tier 1 support to internal Customer users, and this SPOC shall adhere to the roles and responsibilities as follows:
    - Manage the installation of SentinelOne Endpoint Agent software available from the SentinelOne Management Platform Console on all in-scope customer-owned endpoints and manage ongoing updates to that software
    - Manage the installation of SentinelOne Mobile Agent software available from the Apple App Store or Google Play on all in-scope Customer-owned mobile devices and manage ongoing updates to that software
    - Providing secure network transport to transmit information from the agent(s) to the Service

SD-9. Change Control Process

Section Effective Date: 07-Oct-2021

Any changes to the Service shall be handled via the Change Control Process. Either Party must submit change requests to the Service in writing. The party requesting the change must submit a written request on an LevelBlue provided form to the other party and the receiving party will issue a written response within seven (7) days of the receipt of the request, including whether the receiving party accepts or rejects the request. Once agreed both parties must execute the provided form.

SD-10. Use of Service

SD-10.1. Use of the Service

Section Effective Date: 07-Oct-2021

Subject to the requirements, limitations, and restrictions stated in this Service Guide or the Customer Agreement, LevelBlue grants to Customer a limited, non-exclusive, revocable, non- transferable, non-sublicensable right during the applicable Service Term to use the Service (and any Software provided as part of the Service) and Documentation in accordance with the scope of use specified in this Service Guide for Customer's own internal business operations and not for the benefit of any other person or entity. When used in this Service Guide, "Documentation" means user manuals and any other materials, including updates thereto, in any form or medium made generally available by LevelBlue to Customers or Users, regarding the proper installation and use of the Service.

SD-10.2. Requirements, Limitations and Restrictions on Use of the Service

Section Effective Date: 07-Oct-2021

Customer will comply and will cause all Users to comply with the following requirements, limitations and restrictions when accessing or using the Service or Documentation:

- Customer and all Users will not:

- Modify, disclose, alter, translate, or create derivative works of the Service (or any components thereof) or any accompanying Documentation.
- License, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Service (or any components thereof) or any Documentation
- Use the Solutions other than as permitted under this Service Agreement, as directly related to Customer's internal business operations and in conformity with the Documentation, and not otherwise use the Service for any other commercial or business use, including without limitation, offering any portion of the Service as benefits or services to third parties
- Use the Service in violation of any laws or regulations, including, without limitation, to store or transmit infringing, libelous or otherwise unlawful or tortious material, or material in violation of third-party privacy rights.
- Use the Service to store, transmit or test for any viruses, software routines or other code designed to permit unauthorized access, disable, erase or otherwise harm software, hardware, or data, or to perform any other harmful actions
- Probe, scan or test the efficacy or vulnerability of the Service or take any action in an effort to circumvent or undermine the Service, except for the legitimate testing of the Service in coordination with LevelBlue, in connection with considering a subscription to the Service
- Attempt or actually disassemble, decompile or reverse engineer, copy, frame or mirror any part or content of the Service, or otherwise derive any of the Service source code
- Access, test, and/or use the Service in any way to build a competitive product or service or copy any features or functions of the Service
- Interfere with or disrupt the integrity or performance of the Service
- Attempt to gain unauthorized access to the Service or their related systems or networks
- Disclose to any third party or publish in any media any performance information or analysis relating to the Service
- Disclose to any third party any benchmarking or comparative study involving the Service Documentation
- Fail to maintain all copyright, trademark and proprietary notices on the Service and any permitted copy thereof

- Customer is responsible for maintaining the confidentiality of the administrator and User logon identifications, passwords, and account information. Customer will use

commercially reasonable efforts to prevent unauthorized access to or use of Endpoint Security and all Documentation and immediately notify LevelBlue in writing of any such unauthorized access or use or violation by Customer or its Users of the Customer Agreement.

- Customer shall use the Service in accordance with the Documentation and the Acceptable Use Policy
- Customer is solely responsible for the installation of agents in their environment to allow for visibility of its data input and output to the Service and for maintaining a separate means for the reconstruction of any lost data
- To the extent LevelBlue provides Customer with APIs as part of the Service, such APIs are provided "as is" without any warranty of any kind. Customer is granted a personal, non- sublicensable, nonexclusive, nontransferable, limited license to use the API solely for Customer's internal use for exporting Customer's content from LevelBlue to the new Customer system. Customer may not (a) copy, rent, sell, disassemble, reverse engineer, or decompile (except to the limited extent expressly authorized by applicable statutory law), modify, or alter any part of the API; or (b) otherwise use the API on behalf of any third party. The API license shall automatically terminate in the event Customer breaches this section.
- Customer will agree to accept all Enhancements necessary for the proper function of the Service, and that LevelBlue is not responsible for the proper performance of the Service or security issues encountered with the Service related to Customer's failure to accept Enhancements in a timely manner. All use of the Service shall be in accordance with the then-current Documentation. "Enhancements" means any updates, patches, bug fixes and versions to the Service provided to Customer.

SD-10.3. Deployment of Endpoints

Section Effective Date: 07-Oct-2021

Customer agrees to follow LevelBlue's installation instructions for deployment of agent software across the Customer's Endpoints, and that LevelBlue will be given remote access to the Endpoints for the Service, including for the purposes of ascertaining system performance and accessing system logs. Customer agrees that LevelBlue may disclose to third parties' descriptions of security- related activities encountered by Endpoint Security Customer's environment, provided that such descriptions maintain the anonymity of Customer or Users.

SD-10.4. Number of Subscribers

Section Effective Date: 07-Oct-2021

LevelBlue may audit Customer use from time to time to determine if the number of endpoints on the Service has grown above the number of contracted endpoints. In the event the audit reveals that there are more Users than Subscribers, and that Customer has underpaid any Service fees to LevelBlue, Customer will be notified by LevelBlue of such audit results, and will have 30 calendar days to either i) uninstall the additional endpoints or ii) pay to LevelBlue, in accordance with the fees set forth in the Service Agreement, an amount equal to such underpayment.

- The number of endpoints is defined as the number of agent software packages installed on endpoints that can send information to the Service.

SD-10.5. Remote Ops Administrative Tools

Section Effective Date: 12-Dec-2023

Administrative Tools are used with the feature Remote Ops to collect forensic artifacts, execute complex scripts, install and uninstall incident response tools, and more on thousands of endpoints simultaneously.

LevelBlue reserves the right to suspend or terminate this feature if it determines Customer's use of Administrative Tools may cause LevelBlue or a third-party harm or if Customer's use of the Administrative Tools violates the terms this Service Guide.

SD-10.5.1. Restrictions

Section Effective Date: 12-Dec-2023

Customer shall not use Administrative Tools to: (i) perform services, access computers or devices of third parties without their express specific consent, (ii) upload, store or analyze sensitive data to the Service. For the purposes of this provision, “sensitive data” may include, without limitation, payment card industry data, personal information, protected health information, financial data, trade secret, login information and other data that restrict by contract or applicable laws and regulations.

Customer acknowledges that it shall take sole responsibility for any data retrieved using Administrative Tools. Customer acknowledges that Administrative Tools are powerful, highly customizable and can irreparably damage software and hardware and takes sole responsibility for any harm associated with its use of Administrative Tools.

SD-10.5.2. Customer Responsibilities, Representations and Warranties

Section Effective Date: 12-Dec-2023

Administrative Tools are not required for use of the Service and should only be used with caution and by personnel with relevant industry expertise in using similar tools.

Customer represents and warrants that it will exercise the requisite expertise, security measures and due diligence in using Administrative Tools and any data it processes or transfers using Administrative Tools shall be done in accordance with applicable laws or contractual obligations, including without limitation, privacy, data transfer, data export, consent, and contractual obligations and that it has sufficient rights in any data it processes or transfer using Administrative Tools.

LevelBlue reserves the right to remove any data obtained, transferred, or processed by Administrative Tools from the Service to comply with any data retention laws. Otherwise, LevelBlue instructs Customer to delete any Administrative Tool data within 7 days.

SD-10.5.3. Disclaimer

Section Effective Date: 12-Dec-2023

LevelBlue shall have no liability for deletion or corruption of data, loss of access, permanent or temporary downtime on affected systems due to Customer's use of Administrative Tools.

SD-10.5.4. Available Administrative Tools

Section Effective Date: 12-Dec-2023

It is highly recommended that Remote Ops be run fully encrypted. Customer may run Remote Ops unencrypted as long as it accepts full responsibility for the security and retention of any unencrypted data.

SD-10.6. Reservation of Rights; Ownership

Section Effective Date: 07-Oct-2021

Except for the rights expressly granted herein, no other rights, express or implied, are granted to Customer under these terms. All right, title, and interest in and to the Service, the Software and related Documentation are and shall remain the exclusive property of LevelBlue and its licensors.

Customer acknowledges and agrees that: (i) the Service, the Software and related Documentation are protected under U.S. and foreign copyright and other intellectual property laws; (ii) LevelBlue and its licensors retain all copyrights and other intellectual property rights in the Service, the Software and related Documentation; (iii) there are no implied licenses under this license and any rights not expressly granted to Customer hereunder are reserved by LevelBlue; and (iv) Customer acquires no ownership or other interest in the Service, Software, or related Documentation.

SD-11. Service Activation

Section Effective Date: 07-Oct-2021

LevelBlue provides activation for the Service ("Service Activation"). Service Activation will occur when LevelBlue has provisioned the Service. Billing will begin upon the Effective Date of the Service Agreement.

SD-12. Reports

Section Effective Date: 07-Oct-2021

Customer shall own those copies of any reports produced and furnished to Customer by LevelBlue in providing the Service (Reports), and Customer is hereby granted, under LevelBlue's copyrights, the perpetual, non-exclusive, personal, and non-transferable right to reproduce and modify Reports for Customer's own internal business purposes. For avoidance of doubt, "internal business purposes" exclude public distribution, resale to third parties and revenue generation purposes.

SD-13. Customer Data

Section Effective Date: 07-Oct-2021

All rights, title, and interest in and to Customer Data are and will remain the property of Customer and all intellectual property rights including copyright, trademark, and trade secret rights in Customer Data are and will remain the property of Customer. Customer grants to LevelBlue and its licensor, throughout the Term and use of Service and after the Term as necessary for any of LevelBlue's post-termination obligations to Customer, the necessary rights or license to use Customer Data as necessary to perform obligations related to the Service. Customer will not provide to LevelBlue or store as part of its use of the Service Customer Data that includes Payment Card Industry ("PCI") data or Protected Health Information ("PHI") data. Customer shall provide LevelBlue in the form and format and on the schedule specified by LevelBlue, Customer Data as is reasonably required for LevelBlue's performance of the Service. Customer grants to LevelBlue and its licensor a, non-exclusive, non-transferable, non-sublicensable, royalty free license to use such Customer Data in order to provide the Service to Customer and the Users and as necessary to access the Service to monitor and diagnose issues related to the Service, and the ability to use Customer Data to improve the Service. Customer is responsible for maintaining back-up on all Customer Data. "Customer Data" means the data inputted by Customer or its Users for the purpose of using the Service.

SD-13.1. Product Usage Data

Section Effective Date: 07-Oct-2021

Customer agrees that LevelBlue and its licensor may use information about how Customer uses the Service to generate statistics and to otherwise compile, synthesize and analyze such information for the purpose of operating, maintaining, repairing, and improving the Service ("Product Usage Data"). Product Usage Data does not include Customer Data.

SD-14. Data Privacy Disclosure

Section Effective Date: 25-Mar-2023

LevelBlue Endpoint Security requires Customers to share with LevelBlue's supplier, certain User information such as email addresses, names, phone numbers, IP addresses, location data, and other data elements necessary to provide this Service. Additional information regarding the use of data by LevelBlue's supplier in conjunction with LevelBlue Endpoint Security may be found here: https://www.sentinelone.com/legal/privacy-policy/

Customer consents to the collection of this data and agrees to obtain any necessary consents from its Users.

Customer represents and warrants that its use of LevelBlue Endpoint Security will be consistent with applicable privacy laws. Customer must conduct a privacy impact assessment/data protection impact assessment for Users where required by law.

Customer is solely responsible for its relationship with Users and their traffic. Customer has the authority to permit access to communications by its employees, guests, representatives, and other Users and is legally responsible for all consents. Customer represents and warrants that it has the appropriate rights to provide any User data to LevelBlue in connection with the LevelBlue Endpoint Security Service.

SD-15. Cybersecurity Information Sharing Act

Section Effective Date: 25-Mar-2023

LevelBlue provides this Service for a cybersecurity purpose, and in the U.S, both Customer and LevelBlue agree to comply with the Cybersecurity Information Sharing Act of 2015 ("CISA"). When using the Service, Customer agrees to monitoring by LevelBlue and designs and sets all filtering and interception policies ("Security Policies"). LevelBlue undertakes only to implement the Security Policies as directed by Customer and accepts no responsibility for the design or appropriateness of such design or settings. As between LevelBlue and Customer, when using the Service, Customer is solely responsible for obtaining and complying with the authorizations, licenses and permissions required by law or by its suppliers or providers to enable the Service to access data on Customer's applications or products. Customer is responsible for obtaining consent from and giving notice to its Users regarding Customer's and LevelBlue's collection and use of User information in connection with a Service and regarding interception and/or monitoring of communications, including email and Internet use, associated with the Security Policies and the Service. Customer is responsible for obtaining agreement from its Users to provide reasonable cooperation with LevelBlue in connection with responses to requests or requirements regarding the Service by any regulator, authority and/or other governmental entity.

SD-16. Optional Add-On Features

Section Effective Date: 04-Jun-2024

Customer may purchase optional additional features listed below. Individual requirements may apply based upon the feature.

- Ranger - (available with Endpoint Security - Control or Endpoint Security - Complete) - Customer can gain visibility of devices connected to their network. Ranger scans your corporate environment to identify and manage connected devices, even if they are not protected by or supported by a SentinelOne Endpoint Agent.
- Extended Data Retention (only available with Endpoint Security - Complete) - Customer can extend the default data retention period of 14 days and query EDR data for investigating threats or performing threat hunting queries over an extended period.

- Binary Vault (only available with Endpoint Security - Complete) - Customer can upload executable files (malicious or benign) in their environment to SentinelOne Cloud storage and download files on demand (e.g., to run forensic analysis locally or with a third-party sandbox or analysis tool).
- Cloud Funnel (only available with Endpoint Security – Complete) – Customer can securely stream its endpoint telemetry from Deep Visibility to a data lake using a Kafka subscription.
- STAR Pro (only available with Endpoint Security – Complete) – Customer can increase the concurrently active STAR custom rules that turn Deep Visibility queries into automated hunting rules that trigger alerts from 100 rules to 300 rules.
- Remote Ops (only available with Endpoint Security – Complete) – Customer uses Administrative Tools to collect forensic artifacts, execute complex scripts and commands, install and uninstall incident response tools and more on thousands of endpoints simultaneously.

SD-17. Optional Guided Onboarding

Section Effective Date: 04-Jun-2024

Customer may purchase optional Guided Onboarding which provides remote assistance configuring the SentinelOne Management Console and guidance with the deployment of the SentinelOne Endpoint Agents. Customer receives 16 hours of Guided Onboarding assistance with the purchase of the Guided Onboarding Service Component.

SD-17.1. Scope of Guided Onboarding

Section Effective Date: 04-Jun-2024

Guided Onboarding Process

Onboarding Checklist

- Customer provides information on the scope of endpoints and tools used within its environment for the deployment.
- LevelBlue reviews and assesses information provided.

Kickoff Call

- The LevelBlue Project Manager details service onboarding steps.
- LevelBlue and Customer outline roles and responsibilities, contacts, and procedures for document change control requests.

Introduction to LevelBlue Security Engineer

- Project Manager introduces Security Engineer to assist Customer remotely with the remainder of onboarding activities including the planning, implementation, and configuration of the SentinelOne Management Platform.

SentinelOne Management Platform Configuration

- LevelBlue Security Engineer(s) perform SentinelOne Management Platform setup and establish User access.

SentinelOne Agent Deployment

- LevelBlue Security Engineer(s) will recommend a phased approach for Agent Deployment
- Customer is responsible for downloading the Agent installation package, testing the Agent, and deploying the Agent software on all in-scope endpoints per the recommended phased approach.
- LevelBlue Security Engineer will confer with Customer at the end of each phase to track progress and decide on proceeding to the next phase.

Platform Tuning

- LevelBlue Security Engineer will monitor alerts generated to identify any anomalous activity and work with Customer to implement security policies, rules, and/or controls in the SentinelOne Management Platform.

SD-17.2. Guided Onboarding Restrictions and Requirements

Section Effective Date: 04-Jun-2024

Guided Onboarding is available for assistance with Endpoint Security Control or Complete service components and does not apply to Mobile Security, Active Directory Defense, or Identity Threat Detection and Response service components. The 16 hours of Guided Onboarding support must be used within 180 calendar days following the date of the Kickoff Call. Customer forfeits any unused hours. Customer who purchases Guided Onboarding may purchase four hours of Guided Onboarding Additional Hours which are eligible for use during an additional 90 calendar day interval.

SD-17.3. Use of Hours

Section Effective Date: 04-Jun-2024

Commencing upon Customer's engagement with the Guided Onboarding team during the Kickoff Call, time will be deducted from Customer's total hours in 30-minute intervals.

SD-18. Withdrawal of Service or Service Component

Section Effective Date: 25-Mar-2023

LevelBlue may discontinue providing Service upon 12 months' notice, or a Service Component upon 120 days' notice, but only where LevelBlue generally discontinues providing the Service or Service Component to similarly situated Customers.

Service Level Objectives (SLO)

SLO-1. General Endpoint Security and Response SLO Terms

Section Effective Date: 07-Oct-2021

LevelBlue has established performance objectives for Endpoint Security services. Service Level Objectives (SLO) are indicative of the service level LevelBlue strives to meet, but Customer is not entitled to receive any credits for failure to attain an SLO.

The terms below apply to the Service Level Objectives for the SentinelOne Management Platform described in this Service Guide.

- "Maintenance Window" is standard and means Sunday between 10AM UTC +3 and 6PM UTC +3 approximately every 2 weeks. The Service is available at all times except for a downtime during a Maintenance Window or planned downtime which will not exceed six (6) hours per month outside a Maintenance Window of which Customer is notified at least two (2) days in advance though a notice to all Customer's admins through the SentinelOne Platform Management Console.
- "Unscheduled Downtime" for necessary emergency maintenance to address a recently discovered issue in the Service that if left unresolved can materially threaten the security or usability of the Service, which shall be notified to Customer as soon as practically possible or unavailability caused by circumstances beyond reasonable control, such as, but not limited to, acts of God, acts of government, acts of terror or civil unrest, or technical failures beyond control. LevelBlue has no responsibility for the performance and/or availability of 3rd party Internet service providers employed by Customer or any network outside of SentinelOne's control.

SLO-1.1. Endpoint Security Availability Performance Objective

Section Effective Date: 07-Oct-2021

The performance objective for Endpoint Security availability is described below. "Endpoint Security Availability" is measured by the following calculation:

- ((TT - TTF) / TT) x 100 = Percentage (%) of Endpoint Security Availability
    - TT = Total available Minutes per Month (Total minutes in a month – Maintenance = TT). Total available minutes do not include Maintenance.
    - TTF = Total Minutes of Endpoint Security Outage Minutes during the measurement Month

A LevelBlue Endpoint Security Availability Outage shall occur if Customer is unable to access the SentinelOne Management Platform for more than a minute. LevelBlue's objective is to give customers access to the SentinelOne Management Platform at least 99.5% of the time.

Pricing (P)

P-1. Endpoint Security Pricing

Section Effective Date: 07-Oct-2021

Applicable rates, prices, discounts, and other terms for the Service are set forth in the Service Agreement.

Country Specific Provisions (CSP)

P-2. Country Availability

Endpoint Security is available inside and outside the United States.